— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

CT/IB 03/03641

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC, WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JOUX, A.: "A One Round Protocol for Tripartite Diffie-Hellman" LECTURE NOTES IN COMPUTER SCIENCE, vol. 1838, 2000, pages 385-393, XP008026749 page 387, line 1 -page 388, line 10 page 392, line 11 - line 25 --- -/--	1-3,7-16

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 2004	13/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RUBIN K ET AL: "Supersingular abelian varieties in cryptology" , ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2442), ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA , 2002, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 336 - 353 XP002268384 ISBN: 3-540-44050-X cited in the application page 336, line 1 -page 337, last line	1-16
A	VERHEUL E R: "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems" , ADVANCES IN CRYPTOLOGY - EUROCRYPT 2001. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2045), ADVANCES IN CRYPTOLOGY - EUROCRYPT 2001, INNSBRUCK, AUSTRIA, 6-10 M , 2001, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 195 - 210 XP002268385 ISBN: 3-540-42070-3 cited in the application the whole document	1-16